# Content Protection for IEEE 1394 Serial Busses

C. Brendan S. Traw
Staff Systems Architect
Platform Architecture Laboratory
Intel Corporation

brendan_traw@ccm.jf.intel.com

intel®

# Overview

- What is content protection in a IEEE 1394 serial bus context?
  - Scope of protection
  - Digital Transmission Discussion Group (DTDG) goals
- Technical design space
  - Copy Control Information
  - Device Authentication
  - Content Encryption
- An example: Intel's Proposal
- Summary

intel®

# Content Protection for Digital Transmission

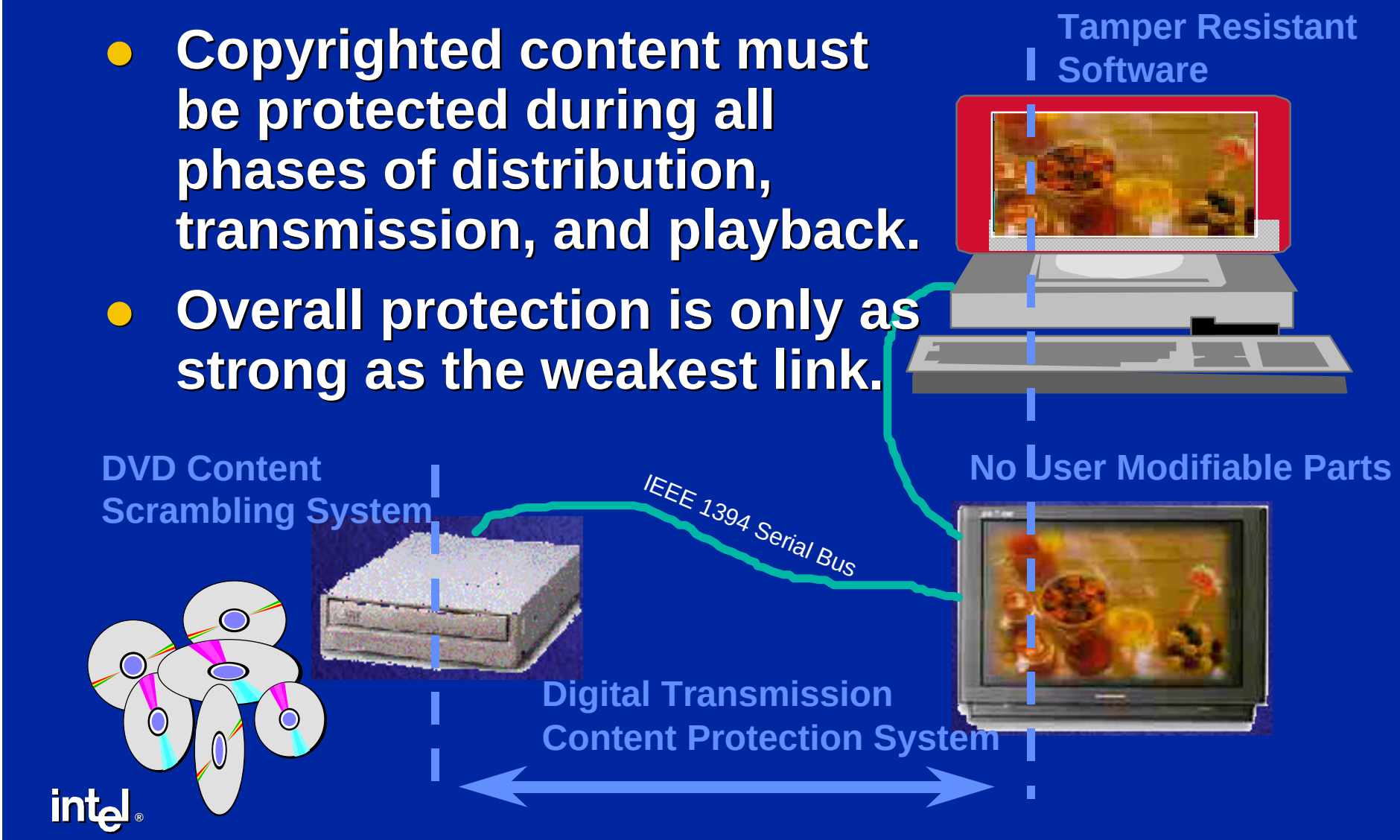
- Overall goal is to ensure that license conditions for copyrighted content are enforceable through technical and legal means
- Provide a robust pipe for content across digital interconnects such as IEEE 1394
- Key enabling technology for digital transport of copyrighted media content


**No digital output of Hollywood content will be allowed without content protection**

intel®

# Content Protection Chain

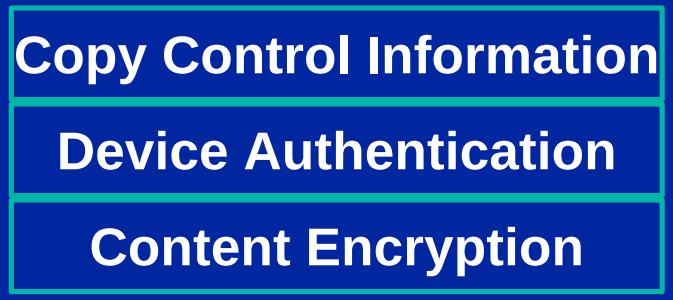
- Copyrighted content must be protected during all phases of distribution, transmission, and playback.
- Overall protection is only as strong as the weakest link.




intel®

# CPTWG Digital Transmission Discussion Group Goals

- Protect copyrighted content traversing digital transmission systems with highest level of technical protection which:
  - Can be implemented with reasonable cost in consumer electronics devices
  - Can be implemented with reasonable processing overhead in software on a PC




intel®

# CPTWG Digital Transmission Discussion Group Goals

- Primary focus on IEEE 1394 Serial Bus
- Copy protection should be transparent to users who comply with the copyright of content
- Licensable, but with no expensive IP
- No import or export problems

# Copy Control Information

- Copy Control Information (CCI) specifies the conditions under which copyrighted content can be copied.
  - Should include support for at least CGMS, APS, and Digital Source bits
- Three forms of CCI:
  - Exposed CCI
    - Carried in Isochronous packet or CIP headers
    - Integrity not guaranteed
    - Typically a subset of full CCI
  - Embedded CCI
    - Carried with content (may be a watermark)
    - Integrity guaranteed through encryption, hashing, or other means
  - Other options
    - Carried “out of band”
    - Integrity guaranteed

intel®

# Device Authentication

- Device Authentication enables a source of content to verify that a potential receiver is a compliant, trusted device
- Universal Secret
  - Devices are authenticated based on knowledge of a secret value which is shared by all devices
  - \+ Simple to implement and fast to perform
  - – Once secret is revealed through reverse engineering of a single device or other means, security of entire system is compromised
- Public Key
  - Devices are authenticated based on their ability to prove that they know a secret which is unique to the device (or model of device) and certified by a license authority
  - \+ No universal secrets or functions are required
  - \+ The compromise of one device does not compromise the robustness of the entire system
  - – Algorithms tend to require more computation and resources to implement

intel®

# Content Encryption

- A cipher is used to encrypt content prior to transmission making it unusable by receiving devices unless the appropriate key is provided
- Block cipher
  - Applies a fixed (key dependent) transformation on a large block of data (e.g. 64 bits)
  - + Typically more efficient for software implementations
- Stream cipher
  - Applies a time-varying (initialized by a key) transformation on individual data units (e.g. bits or bytes)
  - + Typically lower hardware requirements
- Both block and stream ciphers can be fast, cryptographically robust mechanisms for protecting content

intel®

# Well-known vs Proprietary Cryptographic Techniques

## Advantages of well-known cryptographic techniques

- Subjected to scrutiny by academics, industrial researchers, governments, and most importantly, hackers
- Robustness is not based on the secrecy of the algorithms but instead on their inherent strength
- Import/Export permission facilitated since governments are already familiar with the algorithms

## Advantages of proprietary cryptographic techniques

- Algorithms may provide properties not available through better known algorithms
- Developer likely to hold IP

intel®

# An Example Solution: Intel's Proposal

- One of eight proposals submitted to the DTDG
- Device authentication forms the cornerstone of a robust, scaleable framework for protecting content
  - All layers are addressed for completeness
- Based on well known cryptographic algorithms and techniques
- Low resource requirements: Suitable for implementation on PCs and CE devices
- User transparent


intel®

# Support for DTDG Layers

- Device Authentication
  - Two phase process for robustness and user transparency
  - Preliminary Authentication (Universal shared secret)
    - Based on a response to a random challenge which demonstrates knowledge of a universal shared secret
  - Full Authentication (Public key cryptography)
    - Signed exchange of device certificates, random challenges, and cipher key components
    - Uses Digital Signature Standard and Diffie-Hellman Key Exchange

intel®

# Support for DTDG Layers

- Copy Control Information
  - Copy control information can be exchanged between devices via an encrypted control channel or embedded in the data stream
- Content Encryption
  - A wide range of content ciphers can be supported (Blowfish recommended)

# Summary

- Content Protection is required for serial bus devices used for exchanging “Hollywood” Content
- Range of technical solutions possible
- Intel’s Proposal
  - Robust, extensible content protection
  - Suitable for low cost CE and PC implementations
  - User transparent
  - No modifications to IEEE 1394 standards
  - No expensive IP to license
  - No import or export problems

intel®